

CIPHERING DEVICE AND DECIPHERING DEVICE

Patent Number: JP2002190798
Publication date: 2002-07-05
Inventor(s): NINO YUICHI; NAKAMURA NOBUTATSU
Applicant(s): NEC CORP
Requested Patent: ☐ JP2002190798
Application Number: JP20000386556 20001220
Priority Number(s):
IPC Classification: H04L9/16
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To obtain ciphering and deciphering devices capable of reducing the load of ciphering and deciphering processing for various data and applying strong ciphering processing to important data.

SOLUTION: Original data to be the source of data to be transmitted are divided by a data block division means 242 in each sort of data on the basis of an analytical rule 241 stored in an analytical rule storing part 224. Then a data block ciphering means 244 ciphers each data block in accordance with importance on the basis of the contents of the analytical rule 241 to prepare a ciphered data block. A data block integration means 245 integrates the ciphering method of each ciphered data block and the positional information of a storage area storing the ciphered data block as ciphered data and sends the ciphered data to a client. Since ciphering strength can be changed in accordance with the sort of data constituting the original data, efficient ciphering and deciphering processing can be performed and the load of the ciphering device and the deciphering device can be reduced.

Data supplied from the esp@cenet database - 12

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2002-190798

(P2002-190798A)

(43)公開日 平成14年7月5日(2002.7.5)

(51)Int.Cl.⁷

識別記号

F I

データ(参考)

H 0 4 L 9/16

H 0 4 L 9/00

6 4 3

5 J 1 0 4

審査請求 未請求 請求項の数6 O L (全 12 頁)

(21)出願番号 特願2000-386556(P2000-386556)

(22)出願日 平成12年12月20日(2000.12.20)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 仁野 裕一

東京都港区芝五丁目7番1号 日本電気株式会社内

(72)発明者 中村 暢達

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100083987

弁理士 山内 梅雄

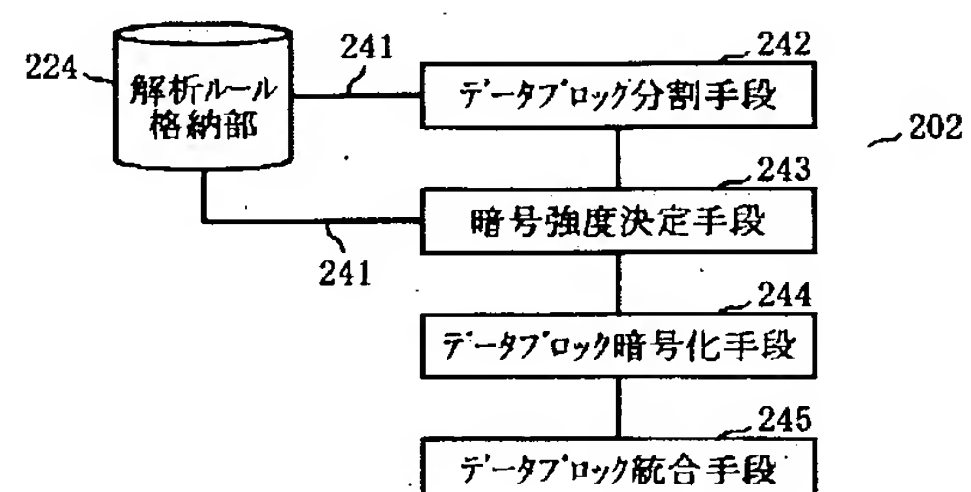
Fターム(参考) 5J104 AA01 AA37 AA38 DA04 JA03
NA02 PA07

(54)【発明の名称】 暗号化装置および復号化装置

(57)【要約】

【課題】 各種データに対して暗号化および復号化の処理の負担を軽減することができると共に重要なデータに対して強度の暗号化処理が可能な暗号化装置および復号化装置を得ること。

【解決手段】 送信するデータの元となる原データは解析ルール格納部224に格納された解析ルール241によって、まずデータの種別別にデータブロック分割手段242で分割される。そして解析ルール241の内容に沿って重要度に応じて、データブロック単位でデータブロック暗号化手段244が暗号化を行い暗号化データブロックを作成する。データブロック統合手段245は暗号化データブロックのそれぞれの暗号化方法と、暗号化データブロックの格納されている記憶領域の位置情報とを暗号化データとして統合し、クライアント側に送出する。原データを構成するデータの種別に応じて暗号化の強度を変えることができるので、効率的な暗号化処理および復号を行うことができ、暗号化装置および復号化装置の負担を軽減できる。



【特許請求の範囲】

【請求項1】 送信すべき原データの重要度をその原データの各部分について判別する重要度判別手段と、この重要度判別手段によって判別した重要度に応じて原データのそれぞれの部分の暗号化の強度を選択する暗号化強度選択手段と、この暗号化強度選択手段によって選択された強度で原データのそれぞれ該当する部分を暗号化する原データ暗号化手段とを具備することを特徴とする暗号化装置。

【請求項2】 送信すべき原データを構成する各部のデータの種別を判別する種別判別手段と、この種別判別手段によって判別された種別ごとに原データをデータブロックに分割する原データ分割手段と、この原データ分割手段によって分割された各データブロックについてこれらを構成するデータの種別を基にして暗号化の強度の重要度を判別する重要度判別手段と、この重要度判別手段によって判別した重要度に応じてそれぞれのデータブロックについての暗号化の強度を選択する暗号化強度選択手段と、この暗号化強度選択手段によって選択された強度でデータブロックごとに暗号化を行う暗号化手段とを具備することを特徴とする暗号化装置。

【請求項3】 送信すべき原データを構成する各部のデータの種別を判別する種別判別手段と、この種別判別手段によって判別された種別ごとに原データをデータブロックに分割する原データ分割手段と、この原データ分割手段によって分割された各データブロックの長さを判別するブロック長判別手段と、このブロック長判別手段によって判別されたブロック長およびデータブロックごとのデータの種別を基にして暗号化の強度の重要度を判別する重要度判別手段と、この重要度判別手段によって判別した重要度に応じてそれぞれのデータブロックについての暗号化の強度を選択する暗号化強度選択手段と、この暗号化強度選択手段によって選択された強度でデータブロックごとに暗号化を行う暗号化手段とを具備することを特徴とする暗号化装置。

【請求項4】 送信すべき原データを構成する各部のデータの種別を判別する種別判別手段と、この種別判別手段によって判別された種別ごとに原データをデータブロックに分割する原データ分割手段と、前記原データ分割手段によって分割されたデータブロックの種別ごとに復号が行われる側での復号の予定時間を検出する復号予定時間検出手段と、この復号予定時間検出手段によって検出された時間に合わせて暗号化の強度を選択する暗号化強度選択手段と、この暗号化強度選択手段によって選択された強度でデータブロックごとに暗号化を行う暗号化手段とを具備することを特徴とする暗号化装置。

【請求項5】 暗号化されたデータを受信してこれをデ

ータの種別別のデータブロックに分割するデータブロック分割手段と、

このデータブロック分割手段で分割したそれぞれのデータブロックを前記暗号化されたデータを受信の際に受信されたデータブロックごとの暗号化方法を示すデータを基にしてデータブロック単位に復号するデータブロック復号手段と、

このデータブロック復号手段によって復号された各データブロックを統合して暗号化する前の原データを再現するデータ統合手段とを具備することを特徴とする復号化装置。

【請求項6】 前記データブロック復号手段は、データブロックごとの暗号化方法を示すデータが暗号化されているか否かを判別する暗号化有無判別手段と、この暗号化有無判別手段が暗号化されていると判別したとき予め取得した暗号鍵を使用して前記データブロックごとの暗号化方法を復号する暗号化方法復号手段を備え、暗号化方法復号手段によって復号された暗号化方法を使用して対応するデータブロックの復号を行うことを特徴とする請求項5記載の復号化装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は暗号化装置および復号化装置に係わり、特に暗号化あるいは復号化の負担を軽減することのできる暗号化装置および復号化装置に関する。

【0002】

【従来の技術】 インターネットに代表される通信ネットワークが広く利用されるようになってきている。またこのような通信ネットワークを使用して通信を行う通信機器として各種のものが登場している。これに伴って、各種のデータがこれらの通信機器によって送受信されるようになってきている。たとえばインターネットおよび携帯型電話機に代表される情報通信端末の発展によって、音楽データ等の各種のデータを格納した種々のサーバから各種の情報通信端末にデータをダウンロードする機会が増えている。

【0003】 これらのサーバの中には前記した音楽データを配信するサーバや、特別に編集された経済情報を会員に配布するサーバのように配布するデータが特定の通信先に限定されているものがある。たとえば有料で音楽データを配布するような場合には、料金を支払う特定の通信先の情報通信端末に限定してデータを送出する必要がある。そこで、このようなデータは暗号化して情報通信端末に送信することで、他の情報通信端末がこれを受信して不当に解読を行わないようにすることが多い。

【0004】 ところが、特に携帯型電話機やPDA (personal digital assistants: 個人向け携帯型情報通信機器) に代表される情報通信端末は通常のパーソナルコンピュータと比較すると搭載するハードウェアの制限等

によって信号の処理能力が低い場合が多い。このため、送出するデータに対して高度な暗号化を行うと、受信した情報通信端末側での復号化のための演算処理に手間取ったり過負荷がかかり他の処理に影響を与えるという不具合が発生するおそれがある。

【0005】そこで、このような問題を解決するための提案が行われている。特開平7-281596号公報に示される第1の提案では、各データ・セグメントについて、複数個の暗号化関数の1つを選択し、選択した暗号化関数を使用してデータ・セグメントを暗号化して、暗号化データ・セグメントを形成している。そして、暗号化データ・セグメントを含む暗号化データ・ブロックを作成し、暗号化データ・ブロックに関して、データを暗号化するために使用された暗号化関数の指示を有する関連した制御ブロックを作成している。

【0006】図17は、特開平7-281596号公報に示される第1の提案の概要を示したものである。この提案では同図(a)に示すように、送信しようとするデータ101を複数個のデータブロック102₁~102_nに分割する。そして、それぞれのデータブロック102₁~102_nに対して順次異なった種類の暗号化を施し、同図(b)に示すように暗号化されたデータブロック103₁~103_nの前に暗号化情報104₁~104_nを配置して、送信を行うようにしている。

【0007】一方、特開平2000-47580号公報記載の第2の提案では、簡単な変換を繰り返し行うことで、複雑な暗号変換を構成する従来の手法に代えて、送信側のサーバと受信側の情報通信端末が異なった複数の暗号アルゴリズムで暗号化あるいは復号化を行う手段を用意している。データの送信を行う前に送信側のサーバと受信側の情報通信端末は、アルゴリズム情報と共通鍵をPKI(Public Key Infrastructure: 認証局サービス)等によって、互いに交換し、その交換された情報に基づいて暗号化したデータをサーバ側から送信し、受信側の情報通信端末で復号化するようにしている。

【0008】これら2つの提案に共通している点は、受信側の情報通信端末が過負荷とならないように、従来と比較すると簡単に復号化できるような簡単なアルゴリズムを使用していることである。そして、他の情報通信端末が暗号アルゴリズムや暗号鍵の推定を容易に行えないようにするために、データの各構成部分あるいは各通信単位でこれら暗号アルゴリズムや暗号鍵を異なるものに行っていることも共通している。

【0009】

【発明が解決しようとする課題】このような提案を採用することによって、受信側の情報通信端末における暗号の解読の負担が多少軽減されることになる。しかし、このような手法を採ると、全てのデータブロックに対して、強度の弱い暗号化方法を採用してしまうこととなるので、データの中でも特に重要な部分が偶然復号化され

てしまう恐れがある。一方で、インターネットで送受信するデータは全て重要であるケースはまれで、特定の重要部分が復号されなければ、他の部分が復号されても、データ送信者にとって不都合とならない場合が多い。例えば、画像データを配信する場合、画像サイズの1ピクセルあたりのデータ長、カラーマップなどを記載したヘッダが復号化されなければ、各画素のデータが仮に復号化されたとしてもクラッカは画像の内容を復元することはできない。

【0010】そこで本発明の目的は、復号化の際の処理の負担を軽減でき、なおかつデータ送信者にとって復号されると不都合な重要なデータについては、強度の暗号化処理を行うことのできる暗号化および復号化装置を提供することにある。

【0011】

【課題を解決するための手段】請求項1記載の発明では、(イ)送信すべき原データの重要度をその原データの各部分について判別する重要度判別手段と、(ロ)この重要度判別手段によって判別した重要度に応じて原データのそれぞれの部分の暗号化の強度を選択する暗号化強度選択手段と、(ハ)この暗号化強度選択手段によって選択された強度で原データのそれぞれ該当する部分を暗号化する原データ暗号化手段とを暗号化装置に具備させる。

【0012】すなわち請求項1記載の発明では、送信すべき原データの重要度をその原データの各部分について判別し、判別した重要度に応じて原データのそれぞれの部分の暗号化の強度を選択するようにしている。そして、これら選択された強度で原データのそれぞれ該当する部分を暗号化することになっているので、重要度の高い部分は十分な強度で暗号化を行うことができる反面、これ以外の一般部分については暗号化の強度を弱くすることができるので、原データの全体に対して画一的に暗号化を強化した場合と比べて全体的な復号化の負担を軽減することができる。

【0013】請求項2記載の発明では、(イ)送信すべき原データを構成する各部のデータの種類の判別する種類判別手段と、(ロ)この種類判別手段によって判別された種類ごとに原データをデータブロックに分割する原データ分割手段と、(ハ)この原データ分割手段によって分割された各データブロックについてこれらを構成するデータの種類の基にして暗号化の強度の重要度を判別する重要度判別手段と、(ニ)この重要度判別手段によって判別した重要度に応じてそれぞれのデータブロックについての暗号化の強度を選択する暗号化強度選択手段と、(ホ)この暗号化強度選択手段によって選択された強度でデータブロックごとに暗号化を行う暗号化手段とを暗号化装置に具備させる。

【0014】すなわち請求項2記載の発明では、送信すべき原データを構成する各部のデータの種類の判別し

て、これら種類に応じて原データをデータブロックに分割するようにしている。そして、分割された各データブロックについてこれらを構成するデータの種別を基にして暗号化の強度の重要度を判別し、判別された重要度に応じてそれぞれのデータブロックについての暗号化の強度を選択し、暗号化を行うようにしている。したがって、原データを構成するデータの種別に応じた強度で暗号化を行うことができ、きめ細かにかつ合理的に暗号化を行うことができるので、復号の際の処理の負担を軽減させることができる。

【0015】請求項3記載の発明では、(イ)送信すべき原データを構成する各部のデータの種別を判別する種別判別手段と、(ロ)この種別判別手段によって判別された種別ごとに原データをデータブロックに分割する原データ分割手段と、(ハ)この原データ分割手段によって分割された各データブロックの長さを判別するブロック長判別手段と、(ニ)このブロック長判別手段によって判別されたブロック長およびデータブロックごとのデータの種別を基にして暗号化の強度の重要度を判別する重要度判別手段と、(ホ)この重要度判別手段によって判別した重要度に応じてそれぞれのデータブロックについての暗号化の強度を選択する暗号化強度選択手段と、(ヘ)この暗号化強度選択手段によって選択された強度でデータブロックごとに暗号化を行う暗号化手段とを暗号化装置に具備させる。

【0016】すなわち請求項3記載の発明では、送信すべき原データを構成する各部のデータの種別を判別して、これら種類に応じて原データをデータブロックに分割するようにしている。そして、分割された各データブロックごとにこれらを構成するデータの種別およびデータブロックの長さに応じた暗号化の強度を選択し、暗号化を行うようにしている。したがって、データブロックの長短を考慮した合理的な暗号化を行うことができ、復号の際の処理の負担を軽減させることができる。

【0017】請求項4記載の発明では、(イ)送信すべき原データを構成する各部のデータの種別を判別する種別判別手段と、(ロ)この種別判別手段によって判別された種別ごとに原データをデータブロックに分割する原データ分割手段と、(ハ)原データ分割手段によって分割されたデータブロックの種別ごとに復号が行われる側での復号の予定時間を検出する復号予定時間検出手段と、(ニ)この復号予定時間検出手段によって検出された時間に合わせて暗号化の強度を選択する暗号化強度選択手段と、(ホ)この暗号化強度選択手段によって選択された強度でデータブロックごとに暗号化を行う暗号化手段とを暗号化装置に具備させる。

【0018】すなわち請求項4記載の発明では、送信すべき原データを構成する各部のデータの種別を判別して、これら種類に応じて原データをデータブロックに分割するようにしている。そして、分割されたデータブ

ックの種類ごとに復号が行われる側での復号の予定時間を検出し、検出された時間に合わせてデータの種別も考慮しながら暗号化の強度を選択するようにしている。したがって、暗号化されたデータを復号する装置側の負荷等を考慮しながら合理的な暗号化を行うことができ、復号の際の処理の負担を軽減させることができる。

【0019】請求項5記載の発明では、(イ)暗号化されたデータを受信してこれをデータの種別別のデータブロックに分割するデータブロック分割手段と、(ロ)このデータブロック分割手段で分割したそれぞれのデータブロックを暗号化されたデータを受信の際に受信されたデータブロックごとの暗号化方法を示すデータを基にしてデータブロック単位に復号するデータブロック復号手段と、(ハ)このデータブロック復号手段によって復号された各データブロックを統合して暗号化する前の原データを再現するデータ統合手段とを復号化装置に具備させる。

【0020】すなわち請求項5記載の発明では、請求項1～請求項4に記載した暗号化装置で暗号化されたデータを復号する復号化装置を扱っている。すなわち、データブロック分割手段は暗号化されたデータを受信してこれをデータの種別別のデータブロックに分割し、データブロック復号手段はそれぞれのデータブロックごとの暗号化方法を示すデータを基にしてデータブロック単位に復号を行う。データ統合手段は復号されたデータブロックを統合して暗号化する前の原データを再現するようにしている。

【0021】請求項6記載の発明では、請求項5記載の復号化装置で、データブロック復号手段は、データブロックごとの暗号化方法を示すデータが暗号化されているか否かを判別する暗号化有無判別手段と、この暗号化有無判別手段が暗号化されていると判別したとき予め取得した暗号鍵を使用してデータブロックごとの暗号化方法を復号する暗号化方法復号手段を備え、暗号化方法復号手段によって復号された暗号化方法を使用して対応するデータブロックの復号を行うことを特徴としている。

【0022】すなわち請求項6記載の発明では、データブロックごとの暗号化方法を暗号化して復号化装置側に送ってきた場合には、予め通信等で取得した暗号鍵を使用してデータブロックごとの暗号化方法を復号し、これを用いて対応するデータブロックの復号を行うことにしている。

【0023】

【発明の実施の形態】

【0024】

【実施例】以下実施例につき本発明を詳細に説明する。

【0025】図1は本発明の一実施例における暗号化装置としてのサーバと復号化装置としての携帯電話機を備えた通信システムの概要を表わしたものである。インターネット201には各種データを格納したサーバ20

2(図では1つのみを例示。)が接続されている。また、インターネット網201は携帯電話網203とも接続されている。携帯電話網203はエリアごとに基地局204(図では1つのみを例示。)と接続されている。基地局204は無線205によって情報通信端末の1つとしての携帯電話機206と接続されるようになっている。

【0026】図2は、図1に示した暗号化装置としてのサーバの構成の概要を表わしたものである。サーバ202はCPU(中央処理装置)221を備えている。CPU221はデータバス等のバス222を通じて各部と接続されている。このうち制御プログラム格納部223、解析ルール格納部224および送信データ格納部225は磁気ディスク(図示せず)の一部の記憶領域で構成できるもので、このうち制御プログラム格納部223にはサーバ202の各種機能を実現するための制御プログラムが格納されている。解析ルール格納部224は後に詳細に説明する暗号化するデータの分割や解析を行うためのルールが格納されている。送信データ格納部225は、送信する各種のデータを格納している。作業用メモリ226は、CPU221の作業に伴って各種の手順やデータを一時的に格納するメモリであり、ランダム・アクセス・メモリ(RAM)によって構成されている。通信制御部227は図1に示したインターネット網201と接続されており、データの送受信を行う回路装置である。

【0027】なお、図1に示した携帯電話機206も図示しないがCPUと、制御プログラムを格納したROM(リード・オンリ・メモリ)および作業用メモリとしてのランダム・アクセス・メモリを備えている。そして、受信したデータを解読して元のデータに再現することができるようになっている。

【0028】図3は、サーバの機能的な構成を示したものである。サーバ202は、図2に示した解析ルール格納部224に格納された解析ルール241を用いてデータの中身を解析してその結果に応じて複数のデータブロックに分割するデータブロック分割手段242と、分割されたそれぞれのデータブロックについての暗号の強度を決定する暗号強度決定手段243を備えている。暗号強度決定手段243は、データの重要度に応じて暗号の強度を決定する。この決定に基づいてデータブロック暗号化手段244はデータブロック単位で暗号化を行い暗号化データブロックを作成する手段である。暗号化データブロックはそれぞれ作業用メモリ226の所定の位置に格納されるようになっている。

【0029】データブロック統合手段245は暗号化データブロックのそれぞれの暗号化方法と、暗号化データブロックの格納されている記憶領域の位置情報と、暗号化データブロックとを暗号化データとして統合する。このようにして統合された暗号化データが送信データとし

て図1に示した携帯電話機206に送出されることになる。以下、これを更に詳しく説明する。

【0030】図4は本実施例で使用するルール情報としての重要部分を特定する情報の一覧を示したものである。図3に示した解析ルール241は、データをそれらの重要度に応じて分割するルールを表わした図4のようなルール情報261から構成されている。ルール情報261は、サーバ202から携帯電話機206に送信する暗号化データの元となる原データの種類ごとに用意されており、解析ルール格納部224に個別に格納されている。本実施例では原データの種類を大きく(1)構造化文書、(2)静止画像、映画等の動画像および(3)その他に分けて、これらの重要部分とそうでない一般部分を区分けしている。

【0031】構造化文書では、タイトルおよび目次部分は重要度が低い一般部分と見なしている。これに対して本文については、重要度の高い重要部分と見なしている。たとえばWWW(world wide web)用の文書記述言語としてのHTML(Hyper Text Markup Language)文書では、図4に示したように「<body>」タグの次から「</body>」タグに至るまでの文書部分を重要部分としている。この部分は本文としてその内容が表示されるからである。これ以外の文書部分は一般部分として重要度を低くしている。

【0032】静止画像については、画像サイズ、ピクセルのサイズ、画像の圧縮方法などが記述されているヘッダ部分は画像を生成する上で重要であるので、重要部分と見なしている。これに対して、各ピクセルの画素の値を記載した箇所は重要度が低い一般部分と見なしている。具体的には図4に示したようにGIF(Graphics Interchange Format)49aフォーマットを例にとると、GIFストリームの開始を示「GIF Header」、「Application Extension」、「Graphic Control Extension」、「Trailer」の部分を重要部分としている。これはこれらの部分はフォーマットならびに記載データが規定されており、一連のデータの中から特定することが可能である。これら以外の部分は一般部分として重要度を低くしている。

【0033】これら以外にも、tiff(Tag Image File Format)やppm(Portable Pix Map)等のように各種の画像ファイルの形式は多数存在する。これらについてはフォーマットが規定されているので、これらを原データ内で特定して重要部分として処理する。これらのヘッダ部分以外は一般部分として重要度を低く設定する。

【0034】JPEG(Joint Photographic Expert Group)およびBMP(Bit Map)ファイルについては、それぞれファイルの先頭から30バイトおよび54バイトがヘッダと規定されている。そこでこれらの部分を特定して重要部分とすることができる。これに対して米国ア

10

20

30

40

50

アップル社の「Quick Time」や、カラー動画画像符号化方式としてのMPEG (Moving Picture Experts Group)、動画と音声を交互に記録するAVI (Audio Video Interleaving) 等の動画画像については、最後の10パーセントにクライマックスシーンが多い。そこで本実施例ではこれらについて原データの最後の10パーセントの部分を重要部分とし、それら以外を一般部分としている。

【0035】その他のファイルとしての以上説明した以外のファイル、たとえば実行可能を示す拡張子「exe」の存在する実行用ファイルについては、そのファイルの内部を解析することは困難である。このため、図4に示したように原データの先頭および末尾のNバイトを重要部分とし、それら以外を一般部分と見なすことにしている。ここで数値Nは正の整数であるが、通常の場合、復号困難なバイト数を確保するという意味で数値Nは8 (バイト) 以上であることが好ましい。このようにデータの先頭および末尾を重要部分としたのは、コンピューターネットワークに不正にアクセスして、データを改ざんしたり破壊する等の行為を行うクラッカがデータを復号するにあたって、対象となるデータの先頭あるいは末尾の部分から作業を開始する可能性が高いからである。

【0036】図4に示した重要部分を特定するルールは原データが解析可能な場合を中心とした解析ルールである。これ以外にも、バイナリデータからそのまま重要部分とそれ以外の一般部分の識別を行うことも可能である。たとえば原データのうちの同じ値が連続する部分は解読されてもクラッカがそのデータを復元しにくい。そこでこのような部分を一般部分とし、それ以外の部分を重要部分とすることができる。このように図4に示した解析ルール格納部224は種々の定義を行うことができる。このため、図4に示した重要部分を特定するルールは、原データの性質に応じて各種の設定が可能であり、図4に示すものに限定されるものではない。

【0037】データブロック分割手段242は、図4に示した重要部分を特定するルールに基づいてサーバ202からクライアントとしての携帯電話機206に送信する原データの内容を解析して、重要度別となったデータブロックに区分けあるいは分割する。

【0038】図5は、このデータブロック分割処理の流れを表わしたものである。図2に示したCPU221は拡張子あるいはファイルの先頭に存在する識別子を基にして、処理の対象となる原データが構造化文書であるかどうかを判別する (ステップS301)。HTML文書に代表される構造化文書であれば (Y)、そのタグを解析する (ステップS302)。そして、これにより重要度別にデータブロックを分割する (ステップS303)。

【0039】一方、同様にしてCPU221が原データ

を静止画であると判別したときには (ステップS304: Y)、ヘッダの解析を行って (ステップS305)、重要度別にデータブロックを分割する (ステップS303)。

【0040】以上と異なり原データが動画画像であると判別したときには (ステップS306: Y)、フレームの解析を行って (ステップS307)、重要度別にデータブロックを分割する (ステップS303)。

【0041】原データが以上のいずれにも該当しない場合には (ステップS306: N)、その先頭と末尾の解析を行う (ステップS308)。そして、図4で示した内容に従って重要度別にデータブロックを分割する (ステップS303)。ステップS303の処理が終了したら、その結果を暗号強度決定手段243に出力して (ステップS309)、データブロック分割処理が終了する (エンド)。

【0042】図6は暗号強度決定手段の処理の流れを表わしたものである。暗号強度決定手段243はデータブロックを1ブロック分読み込み (ステップS321)、そのデータブロックの重要度に応じて暗号アルゴリズムと暗号鍵の長さを決定する (ステップS322)。図4ではデータブロックの重要度を重要部分のとそれ以外の一般部分の2つに分類しているため、データブロック分割手段242で分割されたデータブロックのそれぞれを前記した2つの重要度のいずれかに分類することができる。

【0043】決定された暗号強度が強いほど、暗号としての強度の強いアルゴリズムや長い暗号鍵の選択が行われる。したがって、前記したテーブルは暗号アルゴリズムや暗号鍵の長さを対応付けておくことでそれぞれのデータブロックから暗号アルゴリズムや暗号鍵の長さの決定を簡単に行うことができる。

【0044】このようにして暗号アルゴリズムと暗号鍵の長さが決定されたら、後続のデータブロックが存在しているかどうかをチェックして (ステップS323)、存在していれば (Y)、ステップS321に戻ってその処理を開始する。すべてのデータブロックの処理が終了したら (ステップS323: N)、それぞれの結果をデータブロック暗号化手段244に出力して (ステップS324)、暗号強度決定手段243による処理が終了する (エンド)。なお、暗号強度決定手段243はデータブロックの処理が1つずつ終了するたびにこれらの結果を逐次データブロック暗号化手段244に出力してもよい。

【0045】図7は、データブロック暗号化手段の処理の流れを表わしたものである。データブロック暗号化手段244はデータブロックを1ブロック分読み込み (ステップS341)、指示された暗号アルゴリズムおよび暗号鍵の長さからなる暗号化方法でそのデータブロックを暗号化する (ステップS342)。

【0046】このようにして暗号化データが生成されたら、後続のデータブロックが存在しているかどうかをチェックして（ステップS343）、存在していれば

（Y）、ステップS341に戻ってその処理を開始する。すべてのデータブロックの処理が終了したら（ステップS343：N）、これら暗号化ブロックとこれらに対応する暗号化方法とを組にしてデータブロック統合手段245に出力して（ステップS344）、データブロック暗号化手段244による処理が終了する（エンド）。

【0047】データブロック統合手段245は、データブロック暗号化手段244から出力された暗号化データブロックと、各データブロックにおける暗号化方法およびデータ位置情報が記憶されている暗号化情報ブロックを統合する。そして暗号化データとして出力することになる。ここでデータ位置情報とは、暗号化データブロックの位置を特定するための先頭および末尾のアドレスあるいは先頭のアドレスおよびデータ長からなる情報である。このデータブロック統合手段245の統合の手法は2通り存在する。

【0048】図8は第1の手法で統合された暗号化データの構成を示したものである。第1の手法で統合された暗号化データ401の先頭には、統合された暗号化情報ブロック402が1つ配置されており、これに続いてそれぞれの暗号化データブロック403₁、403₂、……403_mが配置されている。このような暗号化データ401では、暗号化情報ブロック402が先頭に総合された形で配置されているので、復号の処理が簡単になるという長所がある。

【0049】この暗号化情報ブロック402は必ずしも暗号化データ401の先頭に配置する必要はない。すなわち、暗号化情報ブロック402を識別可能にするための特別のフラグを配置したり、あるいは暗号化データ401の先頭に暗号化情報ブロック402の先頭のアドレスを記載しておく等の手法を採ることで任意の位置に配置することが可能になる。

【0050】暗号化情報ブロック402内には、それぞれの暗号化データブロック403₁、403₂、……403_mについての暗号化方法とこれらの先頭アドレスおよび末尾アドレスが格納されている。先頭アドレスはデータの先頭あるいは暗号化データブロック403の終端からのバイト数あるいはビット数で表わされる。末尾アドレスを格納する代わりに、先頭アドレスから末尾アドレスまでのデータ長を格納してもよい。また、クライアントとしての携帯電話機206側に事前に復号鍵を送付していないような場合には、復号鍵もこの暗号化情報ブロック402内に格納することができる。

【0051】図9は第2の手法で統合された暗号化データの構成を示したものである。第2の手法で統合された暗号化データ411は、それぞれの暗号化データブロッ

ク403₁、403₂、……403_mの直前に個別に暗号化情報ブロック412₁、412₂、……412_mを配置している。ただし、それぞれの暗号化データブロック403₁、403₂、……403_mの開始位置を第三者が解読しにくいようにするためには、特開平07-281596号公報にも開示されているように暗号化情報ブロック412と暗号化データブロック403の間に乱数を挿入することも有効である。

【0052】この図9に示した手法では、それぞれの暗号化情報ブロック412₁、412₂、……412_mに、暗号化データブロック403₁、403₂、……403_mのうちの対応するものの暗号化情報およびデータ長を格納することになる。暗号化情報ブロック412₁、412₂、……412_mのデータ長が可変であったり、暗号化情報ブロック412₁、412₂、……412_mと暗号化データブロック403₁、403₂、……403_mのうちの対応するものとの間に何らかのダミーデータが挿入されているような場合がある。このような場合には、先頭アドレスあるいは末尾アドレスのいずれかをデータ長に加えたり、あるいはデータ長自体は記録せずに先頭アドレスと末尾アドレスの双方を記録するようにすればよい。この第2の手法でも、第1の手法と同様に、携帯電話機206側に事前に復号鍵を送付していないような場合には、暗号化情報ブロック402内に復号鍵を格納することができる。

【0053】以上の第1の手法と第2の手法いずれの場合でも、暗号化情報ブロック402、412₁、412₂、……412_mとして暗号化していないデータを使用することもできるし、セキュリティを高めるためにサーバ202と携帯電話機206の間で事前に取り決めた暗号アルゴリズムで暗号化したデータを使用することもできる。

【0054】図10は携帯電話機側の復号化装置の構成の概要を表わしたものである。図1に示したクライアントとしての携帯電話機206は、インターネット網201、携帯電話網203および基地局204を介して受信した暗号化データ401（411）からデータブロックを分割するデータブロック分割手段501を備えている。データブロック分割手段501で分割された個々のデータブロックは、データブロック復号手段502で復号化され、データ統合手段503によって原データに統合されるようになっている。

【0055】なお、データブロック分割手段501、データブロック復号手段502およびデータ統合手段503は、サーバ202側の図3で示した各手段と同様に図示しないCPUとこれが実行するプログラムによって機能的に実現する手段である。もちろん、これらの一部または全部をハードウェアで実現することも可能である。

【0056】図11はデータブロック分割手段の処理の流れを表わしたものである。携帯電話機206は暗号化

データ401(411)を受信すると(ステップS521:Y)、暗号化情報ブロックが暗号化されているかどうかを事前の取り決め内容等によって判別する(ステップS522)。暗号化されている場合には(Y)、図8または図9に示した暗号化情報ブロック402(412₁、412₂、……412_m)を復号化する(ステップS523)。そして、暗号化情報ブロック402(412₁、412₂、……412_m)の内容に基づいて、暗号化データを元の複数の暗号化データブロック403₁、403₂、……403_m(図8、図9参照)に分割する(ステップS524)。暗号化情報ブロック402(412₁、412₂、……412_m)を暗号化していない場合には(ステップS522:N)、直ちにステップS524の処理が行われる。ステップS524の処理が終了したら、暗号化データブロック403₁、403₂、……403_mをデータブロック復号手段502に出力して(ステップS525)、データブロック分割手段501の処理を終了させる(エンド)。

【0057】図12は、データブロック復号手段の処理の流れを表わしたものである。データブロック復号手段502は、データブロック分割手段501から入力された暗号化データブロック403₁、403₂、……403_mに暗号鍵が添付されているかどうかを判別し(ステップS541)、添付されている場合にはその暗号鍵を使用して暗号化データブロック403₁、403₂、……403_mを復号する(ステップS542)。このとき、暗号化情報ブロック402(412₁、412₂、……412_m)に格納されている対応する暗号化方法に基づいてこれらの暗号化データブロック403₁、403₂、……403_mを復号することになる。特開平2000-47580号公報に開示されているように、暗号鍵を所定の方法(たとえばPKIあるいはDiffie-Hellman法)で事前に交換している場合には、(ステップS541:N)、事前に得られたその暗号鍵を使用し、暗号化情報ブロック402(412₁、412₂、……412_m)に格納されている対応する暗号化方法に基づいてこれらの暗号化データブロック403₁、403₂、……403_mを復号する(ステップS543)。

【0058】ステップS542あるいはステップS543の処理がすべての暗号化データブロック403₁、403₂、……403_mについて終了したら、データブロック復号手段502は復号された各データをデータ統合手段503に出力することになる(ステップS544)。

【0059】図13は、データ統合手段の処理の流れを表わしたものである。データ統合手段503は各ブロックごとのデータを1つずつ統合し(ステップS561)、統合するデータが存在する間はこの手順を繰り返す(ステップS562:N)。すべてのデータの統合が終了したら(Y)、これによって復元された原データを、携帯電話機206(図1)の文字や映像等の情報再

生用の領域あるいは回路装置(図示せず)に出力することになる(ステップS563)。

【0060】以上説明した実施例ではデータブロック分割手段242が2種類のデータブロックに分割し、このうちの重要部分のデータブロックには暗号強度の強い暗号化手法を採用し、これ以外の一般部分のデータブロックについては暗号強度の弱い暗号化手法を採用した。これにより従来と比べると重要部分のセキュリティを充分向上させることができる。もちろん、図4に示したルール情報を複数の重要度に区分けしておけば暗号化強度を多段階に設定することができる。

【0061】発明の第1の変形例

【0062】図14は、本発明の第1の変形例におけるサーバの構成の概要を表わしたものである。この図14で先の実施例の図3と同一部分には同一の符号を付しており、これらの説明を適宜省略する。第1の変形例のサーバ202Aのデータブロック分割手段242は、解析ルール格納部224に格納された解析ルール241を用いてデータの中身を解析し、原データを複数のデータブロックに分割してブロック長検出手段601に出力するようになっている。ブロック長検出手段601はこれらのデータブロック長を検出し、暗号強度決定手段243Aは検出されたデータブロック長に応じて暗号化の強度を調整する。

【0063】たとえば、データブロック長の短いものについては暗号アルゴリズムが弱いと簡単にデータを復元されてしまう危険性がある。そこで、このようなものについては暗号の標準方式の1つとしてのTriple DES (Triple Data Encryption Standard) のように比較的暗号強度の強いものを選択する。また、中程度のデータブロック長の場合にはDES (Data Encryption Standard) のような中程度の暗号化強度を選択する。データブロック長の長いもの場合にはDESの攪乱回数を少数にしたもののように暗号強度の比較的弱いものを選択する。このような暗号化強度のきめ細かな選択によって、データブロック暗号化手段244はそれぞれのデータブロックに応じた適切な暗号化を行うことができる。

【0064】これにより、データのセキュリティを比較的高く保ちながら、携帯電話機206側では暗号強度の比較的弱いものについては復号に際する負担を軽減することができ、全体としての復号に要する時間を従来よりも短縮することができる。

【0065】発明の第2の変形例

【0066】図15は、本発明の第2の変形例におけるサーバの構成の概要を表わしたものである。この図15で第1の変形例の図14と同一部分には同一の符号を付しており、これらの説明を適宜省略する。第2の変形例のサーバ202Bは、第1の変形例のサーバ202Aと同様にデータブロック長の検出を行うブロック長検出手

10

20

30

40

50

段601を備えている。このブロック長検出手段601の検出結果は復号予定時間検出手段621に入力されるようになっている。

【0067】図16は復号予定時間検出手段の処理の流れを表わしたものである。復号予定時間検出手段621は原データの種別に応じて復号予定時間の検出を行う。原データが動画の場合には（ステップS641：Y）、33msec（ミリ秒）に設定する（ステップS642）。アニメーションGIF（Graphics Interchange Format）の場合には（ステップS643：Y）、データの内部に記載されている表示間隔によって復号予定時間を規定する（ステップS644）。これ以外の場合、すなわち原データが静止画やテキスト情報の場合には（ステップS643：N）、デコード時間に違和感が無い程度の時間として一例として復号予定時間を3秒に設定する（ステップS645）。このようにして復号予定時間が検出されたらこれを暗号強度決定手段243Bに出力する（ステップS646）。本実施例の暗号強度決定手段243Bは図15に示すように復号速度データ格納部622から復号速度データ623の供給も受けるようになっている。

【0068】図15に戻って説明を続ける。暗号強度決定手段243Bでは、復号速度データ格納部622から供給された復号速度データ623に基づいて各データブロックの暗号強度を調整する。復号速度データ623は、クライアントとしての携帯電話機206でサポートしている暗号化方法のすべてについてデコード速度 V_i （バイト/sec）を事前に測定して得られたデータであり、復号速度データ格納部622に格納されている。ここで符号 i は、暗号化方法を特定するためのインデックスを示している。

【0069】暗号強度決定手段243Bは、復号予定時間を T （sec）、また各データブロック長を L_j としたとき、次の（1）式を満足するように各データブロックの暗号化方法を決定する。ここで符号 j は、暗号化方法を特定するためのインデックスを示している。

【0070】

【数1】

$$T = \sum_i \frac{L_j}{V_i} \quad \dots\dots (1)$$

【0071】暗号化方法の決定については、各データブロックの重要度を拘束条件とした線形計画法を使用して最適な暗号化手法を計算することが可能である。しかしながら、このような手法に限定されるものではなく、重要部分で暗号強度が強く、その他の一般部分で暗号強度が弱くなっていれば、他の手法も利用可能である。このようにして決定された各データブロックの暗号化方法は解析データ記憶手段624に順次格納される。

【0072】データブロック暗号化手段244Aは、解析データ記憶手段624に格納されている暗号化方法で

それぞれ対応するデータブロックの暗号化を行う。データブロック統合手段245は暗号化されたデータブロックと各データブロックにおける暗号化方法およびデータ位置情報が記憶されている暗号化情報ブロックを統合する。そしてこれを暗号化データとして出力することになる。

【0073】この第2の変形例によれば、クライアントでサポートしている全暗号化方法のデコード速度を予め測定しておき、データブロックに応じて暗号化方法を適応的に選択している。このため、復号予定時間に合わせて復号化データを作成することが可能になる。

【0074】なお、実施例および変形例では携帯電話機を例に挙げて説明したが、本発明の暗号化および復号化の適用される装置はこれに限られるものではなく、PHS（Personal Handyphone System）、PDAその他の情報通信端末を含むものであることは当然である。

【0075】

【発明の効果】以上説明したように請求項1～請求項4記載の発明によれば、送信すべき原データを構成する各部分の重要度に応じて暗号化の強度を選択することにしたので、例えば一部のみ重要なデータについてはその部分のみ暗号化の強度を高めればよく、復号化の際の処理を全体的に迅速に行わせることができるという効果がある。

【0076】また請求項2～請求項4記載の発明によれば、送信すべき原データを構成する各部のデータの種別を判別して、暗号化の強度をこれに応じて定めているので、処理が画一的で簡単になるという利点がある。

【0077】更に請求項3記載の発明では、ブロック長判別手段によって判別されたブロック長を勘案して暗号化の強度の重要度を判別するので、よりきめ細かな暗号化を行うことができ、復号の際の処理の負担を軽減させることができる。

【0078】また請求項4記載の発明によれば、分割されたデータブロックの種別ごとに復号が行われる側での復号の予定時間を検出し、検出された時間に合わせてデータの種別も考慮しながら暗号化の強度を選択するようにしているので、暗号化されたデータを復号する装置側の負荷等を考慮しながら合理的な暗号化を行うことができ、復号の際の処理の負担を軽減させることができる。

【0079】更に請求項5記載の発明によれば、暗号化されたデータを受信してこれをデータの種別別のデータブロックに分割し、それぞれのデータブロックごとの暗号化方法を示すデータを基にしてデータブロック単位に復号するので、重要度の低いデータブロックについての処理が大幅に軽減され、全体的な処理の負担を軽減したり、処理の速度を向上させることができる。

【0080】また請求項6記載の発明によれば、予め取得した暗号鍵を使用してデータブロックごとの暗号化方法を復号し、これを用いて対応するデータブロックの復

号を行うので、データのセキュリティを充分確保することができる。

【図面の簡単な説明】

【図1】本発明の一実施例における暗号化装置としてのサーバと復号化装置としての携帯電話機を備えた通信システムの概要を表わしたシステム構成図である。

【図2】図1に示した暗号化装置としてのサーバの構成の要部を表わしたブロック図である。

【図3】本実施例のサーバの機能的な構成を示したブロック図である。

【図4】本実施例で使用するルール情報としての重要部分を特定する情報の一覧を示した説明図である。

【図5】本実施例のデータブロック分割処理を表わした流れ図である。

【図6】本実施例の暗号強度決定手段の処理を表わした流れ図である。

【図7】本実施例のデータブロック暗号化手段の処理を表わした流れ図である。

【図8】本実施例で第1の手法で統合された暗号化データの構成を示した説明図である。

【図9】本実施例で第2の手法で統合された暗号化データの構成を示した説明図である。

【図10】本実施例でクライアントとしての携帯電話機側の復号化装置の構成の概要を表わしたブロック図である。

【図11】本実施例でデータブロック分割手段の処理を表わした流れ図である。

【図12】本実施例でデータブロック復号手段の処理を表わした流れ図である。

【図13】本実施例でデータ統合手段の処理を表わした流れ図である。

【図14】本発明の第1の変形例における暗号化装置と

してのサーバの構成の要部を表わしたブロック図である。

【図15】本発明の第2の変形例における暗号化装置としてのサーバの構成の要部を表わしたブロック図である。

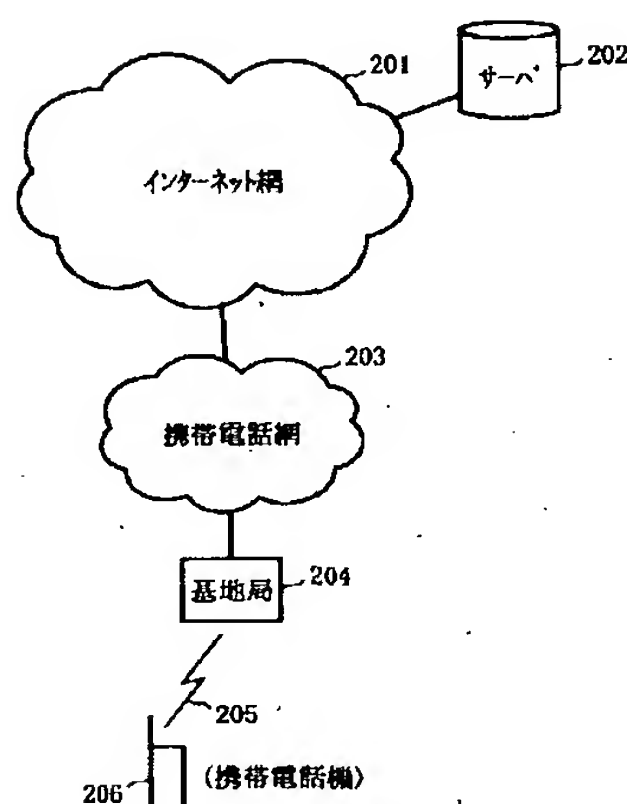
【図16】第2の変形例における復号予定時間検出手段の処理の流れを表わした流れ図である。

【図17】暗号化されたデータの復号化を簡略化することのできる第1の提案の概要を示した説明図である。

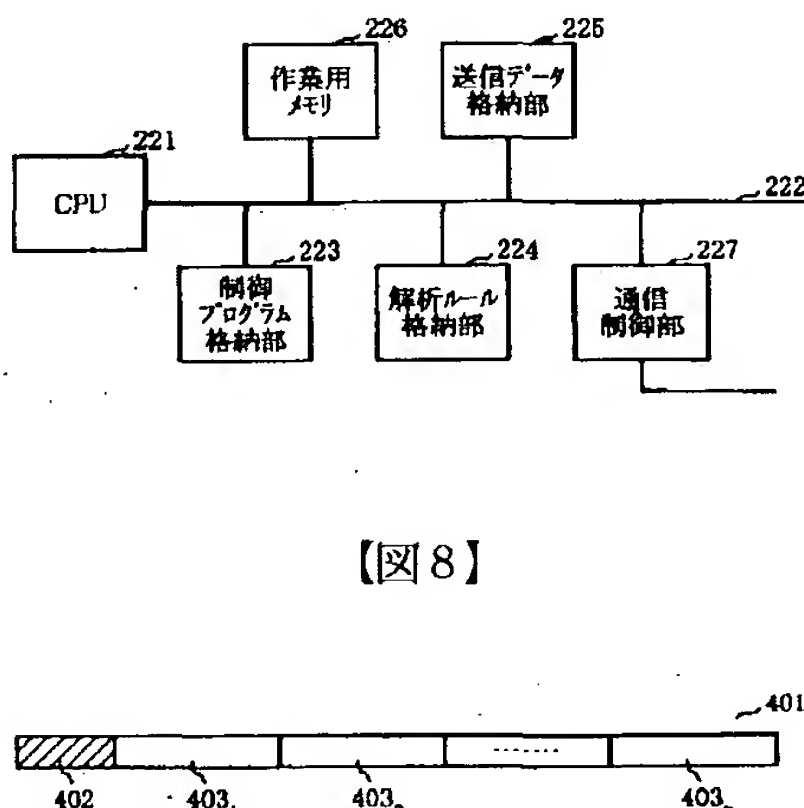
10 【符号の説明】

- 201 インターネット網
- 202、202A、202B サーバ
- 206 携帯電話機（情報通信端末）
- 221 CPU（中央処理装置）
- 223 制御プログラム格納部
- 224 解析ルール格納部
- 241 解析ルール
- 242 データ分割手段
- 243、243A、243B 暗号強度決定手段
- 20 244、244A データブロック暗号化手段
- 245 データブロック統合手段
- 401、411 暗号化データ
- 402、412 暗号化情報ブロック
- 403 暗号化データブロック
- 501 データブロック分割手段
- 502 データブロック復号手段
- 503 データ統合手段
- 601 ブロック長検出手段
- 621 復号予定時間検出手段
- 622 復号速度データ格納部
- 624 解析データ記憶手段

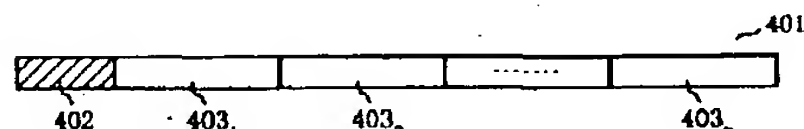
【図1】



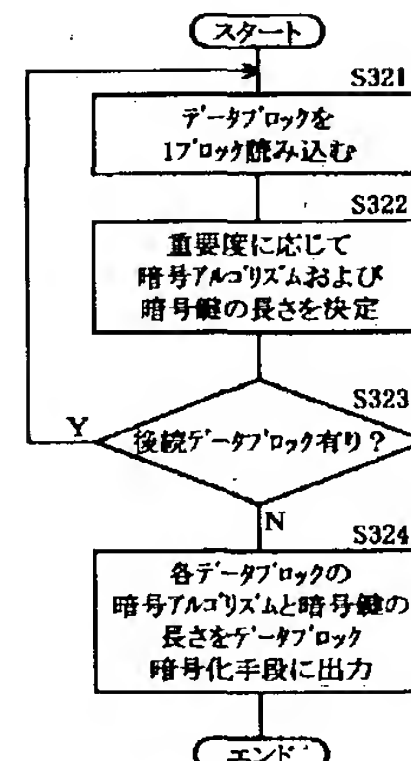
【図2】



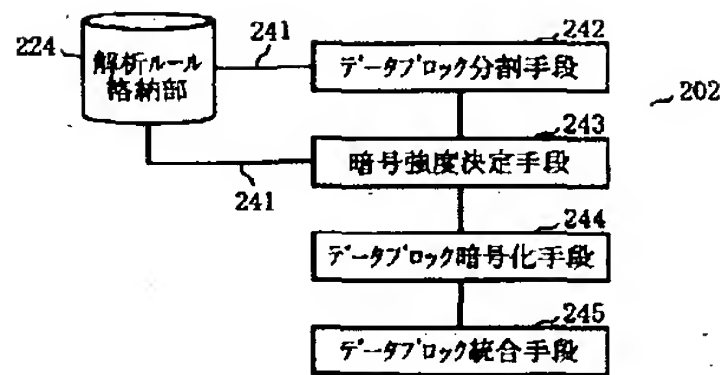
【図8】



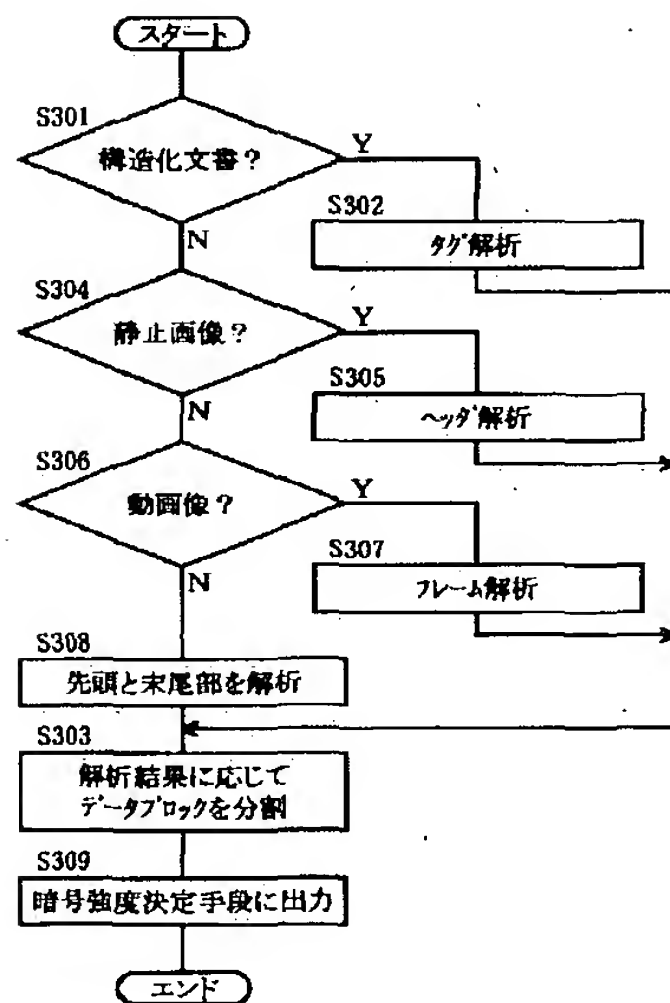
【図6】



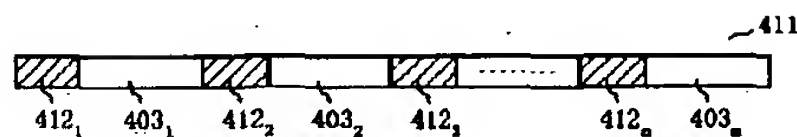
【図3】



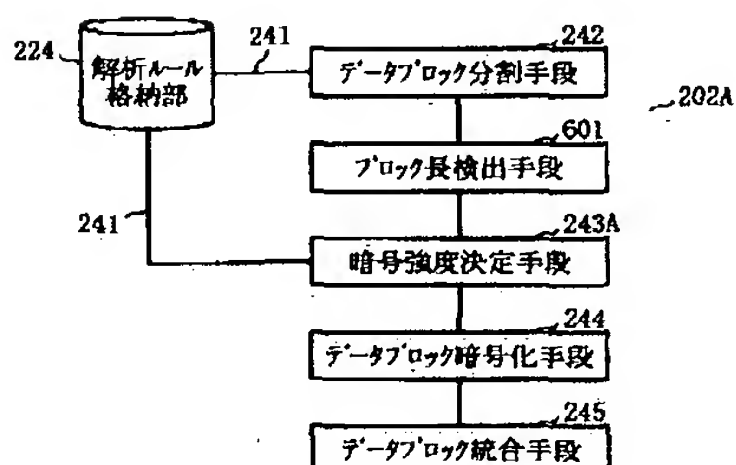
【図5】



【図9】



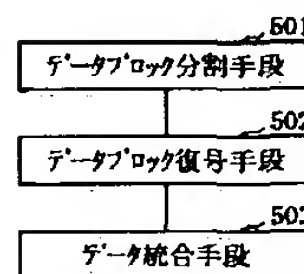
【図14】



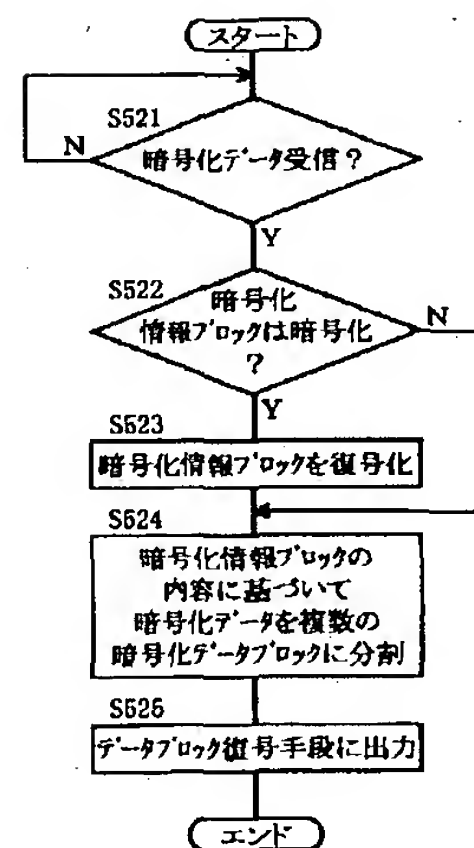
【図4】

データ種類	重要部分
HTML	<body></body>
...	...
GIF 94a	GIF Header, Application Extension, Graphic Control Extension, Trailer
JPEG	先頭から30byte
BMP	先頭から54byte
...	...
Quick Time, MPEG, AVIなど	データの最後の10%
その他	データの先頭と末尾のN byte

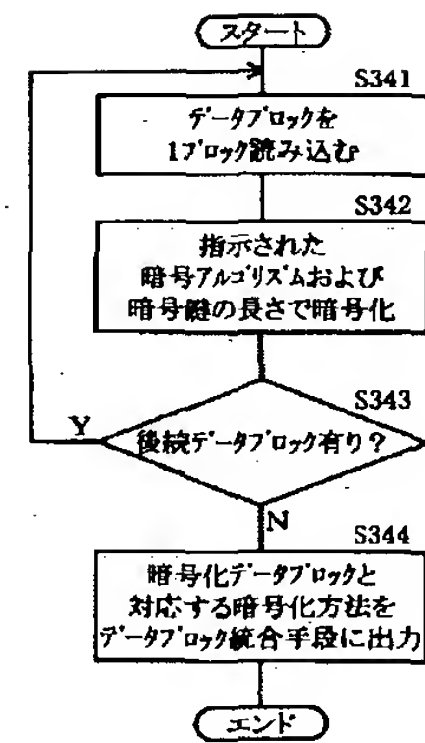
【図10】



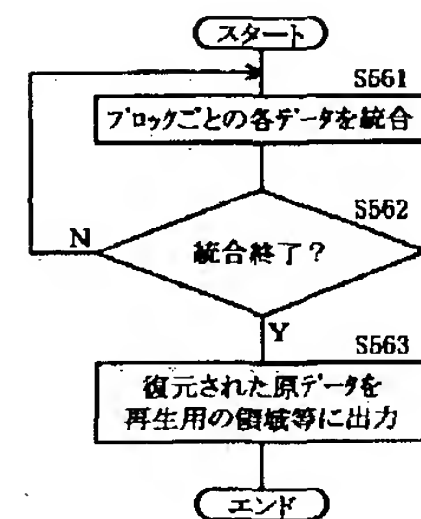
【図11】



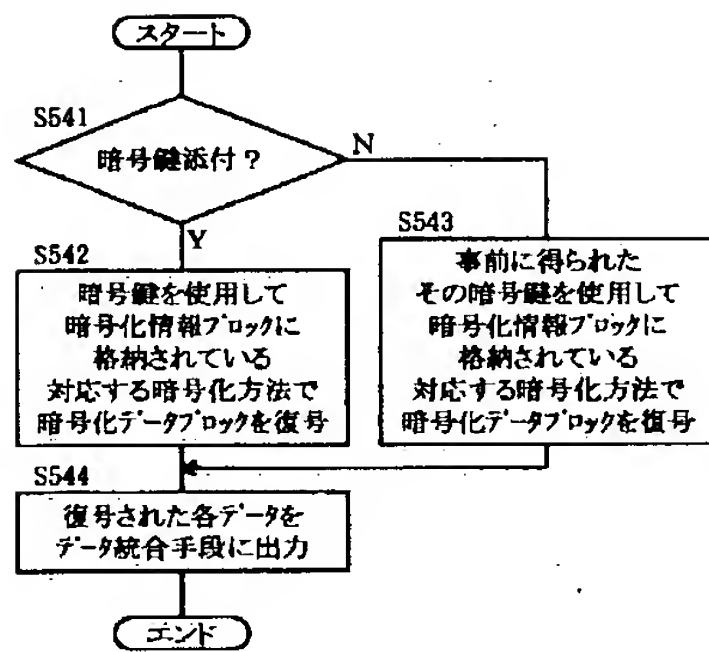
【図7】



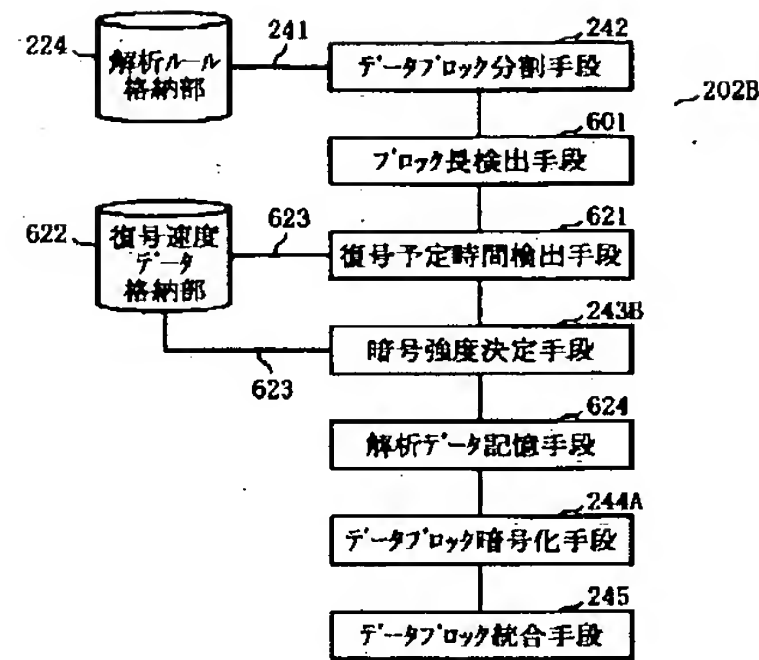
【図13】



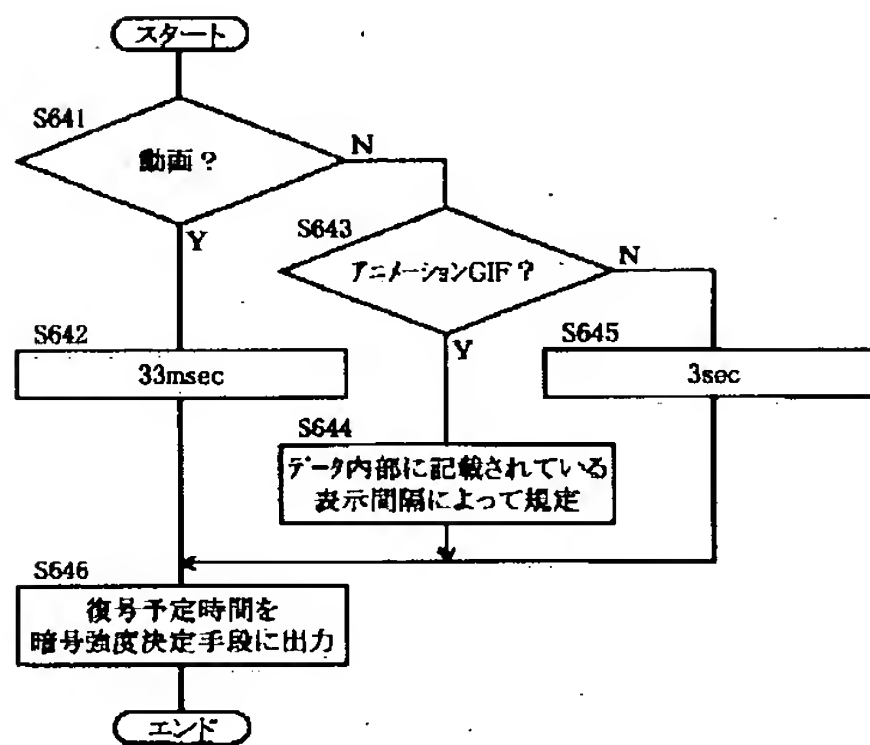
【図12】



【図15】



【図16】



【図17】

